Attorney Docket No.: 5577-237

METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR AUTHENTICATION BETWEEN CLIENTS AND SERVERS USING DIFFERING AUTHENTICATION PROTOCOLS

Field of the Invention

The present invention relates to authentication and more particularly to authentication of messages where a principal and a resource utilize different security protocols.

Background of the Invention

Networked computer applications are often deployed using a "tiered" model. In this model, the originator of a request for a unit of work (also referred to as a "principal") typically initiates that work via a client program (first tier), which then communicates to a web server, or similar second tier server (also referred to as a middle-tier server), which itself communicates, on behalf of the request originator, to other middle-tier servers and/or to third or fourth tier servers such as database servers or other resource managers. When the request is processed by the resource managers, they, typically, evaluate whether the request originator has been authenticated and whether the originator is authorized to perform the unit of work. The resource managers, typically, also record access by the originator of the request in appropriate audit logs.

Such a tiered approach to networked applications may create a need for the secure propagation of security credentials of the request originator through each of the tiers of the application. In such propagation of secure credentials, the request originator delegates to the middle-tier servers the authority to access other servers on their behalf. Thus, the secure propagation of the credentials of the request originator (the requesting "principal") may be referred to as "delegation" or "impersonation."

One security mechanism that provides for delegation is Kerberos. In Kerberos, the requesting principal sends the request accompanied by a delegatable service ticket obtained from a trusted third party, the Kerberos key distribution center. The middle-tier server then uses the delegatable service ticket to obtain service tickets from the key distribution center. The obtained service tickets are used to impersonate the requesting principal to other servers in the network as needed to satisfy the original request.

The Kerberos approach to delegation, however, is intended primarily to handle synchronous connection to other servers and may not extend well to cases when the request is passed as an asynchronously transmitted message. A conventional approach for asynchronous message based authentication is to create a digital signature for the message. The digital signature is based on a public/private key pair. An example of such a digital signature approach to authentication is Public Key Infrastructure (PKI) authentication. PKI authentication is also conventionally used for synchronous connections, as in for example, Secure Socket Layer (SSL) and Transport Layer Security (TLS).

Summary of the Invention

Embodiments of the present invention provide methods, systems, and computer program products for authenticating a message that is sent from an intermediate principal, such as a middle tier server, to a resource manager, where a client originates a request via a message to the intermediate principal using one authentication protocol, and where a different message is sent to the resource manager by the intermediate principal on the client's behalf, and where this second message is authenticated by a different authentication protocol. The message issued by the client containing the original request, *i.e.* a first message, may be referred to herein as the "C-message." The message issued by the intermediate principal on the client's behalf and carrying the delegated authority of the client, *i.e.* a second message, may be referred to as the "D-message." Note that each of the C-message or the D-message or both may constitute all or part of an asynchronous transmission, or may constitute all or part of a synchronous data connection. The D-message includes information from the client which has been authenticated by the intermediate principal using the first authentication protocol. In addition to this information, the D-message carries authentication information of the second authentication protocol, and is authenticated by the resource manager using that protocol.

In particular embodiments of the present invention, the first authentication protocol is Kerberos and the second authentication protocol is public key authentication s is enabled by a public key infrastructure (PKI). In such embodiments, authenticating the D-message may be provided by signing the D-message with a private key corresponding to a PKI certificate available to the resource manager. Furthermore, the D-message may be generated by receiving a Kerberos ticket, verifying authenticity of the Kerberos ticket and extracting principal information from the Kerberos ticket if the authenticity of the ticket is verified. The D-message is then generated utilizing the extracted principal information.

In further embodiments of the present invention, the D-message is generated utilizing the extracted principal information by incorporating the principal information with data from the message from the client to provide the D-message. In such embodiments, the resource manager receives the D-message and authenticates the signature of the D-message. The principal information is extracted from the D-message and the data of the D-message processed based on the principal information from the D-message if the signature of the D-message is authentic. Note that the resource manager determines whether or not the unit of work is authorized based on the identify of the client, not the identity of the middle-tier server or that of the public key signature service. The resource manager, typically, must recognize associated with the D-message signature as a trusted signature service, although the permissions granted tot he identity of the middle-tier server may be different from the permissions granted to the client identity by the resource manager.

In alternative embodiments of the present invention, the D-message is generated utilizing the extracted principal information by generating at least a first component and a second component of the D-message. The first component contains the principal information and the second component contains data from the message from the client. For example, the first component may contain the principal information that identifies the client and the second component contain the request data from the C-message. In such embodiments, the D-message is signed with a private key by signing the first component with the private key and signing the second component with the private key. Furthermore, the resource manager receives the D-message, authenticates the signatures of the first component and the second component, extracts the principal information from the first component and extracts the data, such as the request data from the C-message, from the second component. The request data of the second component is processed based on the principal information from the first component if the signatures of both components of the D-message are authentic.

In additional embodiments of the present invention, the Kerberos ticket and the request data from the C-message are sent from a middle-tier server to a public key signature service. In such embodiments, the public key signature service signs the message, so that it can be authenticated by the resource manager, and returns the signed D-message to the middle-tier server so that middle-tier server can forward it to the resource manager. Furthermore, data flows between the middle-tier server and the public key signature service may be authenticated, for example, using Data Encryption Standard (DES), SSL or other such mechanisms for encrypted data communications.

In still further embodiments of the present invention, the Kerberos service ticket is obtained by the middle-tier server responsive to receiving a delegatable Kerberos ticket. Also, an identification of the middle-tier server may be incorporated in the D-message as this information may be used to trace the delegation of authority from the client to the middle-tier server so as to associate the unit of work with the identities of both the client and the middle-tier server.

In still further embodiments of the present invention, a system for authentication of messages from a client utilizing Kerberos authentication and a resource manager utilizing public key infrastructure (PKI) authentication is provided by a public key signature service configured to receive a Kerberos service ticket, authenticate the Kerberos service ticket, generate a message incorporating data associated with the authenticated Kerberos service ticket which is signed using a digital signature based on a PKI private key and PKI certificate so as to allow the resource manager to authenticate the message and provide the signed message to the resource manager.

In additional embodiments of the present invention, the public key signature service is further configured to extract principal information from the Kerberos service ticket and incorporate the principal information with the message.

The system may also include a middle-tier server configured to obtain the Kerberos service ticket responsive to receipt of a delegatable Kerberos ticket and to provide the obtained Kerberos service ticket to the public key signature service. In such embodiments, the public key signature service may be further configured to provide the signed message to the resource manager by returning the signed message to the middle-tier server. The middle-tier server may be further configured to forward the signed message returned by the public key signature service to the resource manager.

In further embodiments of the present invention, the public key signature service is further configured to extract middle-tier server information from the Kerberos service ticket and incorporate the middle-tier server information with the message. The public key signature service may also be configured to selectively incorporate the principal information into the message with the data associated with the Kerberos service ticket and to selectively generate a second message associated with the message containing the data associated with the Kerberos ticket which contains the principal information and sign the message containing the data and the second message if the second message is generated.

As will further be appreciated by those of skill in the art, while described above primarily with reference to method aspects, the present invention may be embodied as methods, apparatus/systems and/or computer program products.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating a system incorporating embodiments of the present invention;

Figure 2 is a block diagram of a data processing system suitable for use as a public key signature service, middle tier server, client and/or server according to embodiments of the present invention;

Figure 3 is a more detailed block diagram of a public key signature service according to embodiments of the present invention;

Figure 4 is a flowchart illustrating operations of a middle-tier server according to embodiments of the present invention;

Figure 5A is a flowchart illustrating operations of a public key signature service according to embodiments of the present invention;

Figure 5B is a more detailed flowchart of operations of **Figure 5A** according to further embodiments of the present invention; and

Figure 6 is a flowchart illustrating operations of a resource manager according to embodiments of the present invention.

Detailed Description of the Invention

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which illustrative embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

As will be appreciated by one of skill in the art, the present invention may be embodied as a method, data processing system, or computer program product.

Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects all generally referred to herein as a "circuit" or "module." Furthermore, the present invention may take the form of a computer program product on a computer-usable storage medium having computer-usable program code embodied in the medium. Any suitable computer readable medium may be utilized including hard disks, CD-ROMs, optical storage devices, a transmission media such as those supporting the Internet or an intranet, or magnetic storage devices.

Computer program code for carrying out operations of the present invention may be written in an object oriented programming language such as Java®, Smalltalk or C++. However, the computer program code for carrying out operations of the present invention may also be written in conventional procedural programming languages, such as the "C" programming language. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer. In the latter scenario, the remote computer may be connected to the user's computer through a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

The present invention is described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

Various embodiments of the present invention will now be described with reference to the figures. As will be appreciated by those of skill in the art in light of the present disclosure, while embodiments of the present invention are described primarily with reference to Kerberos and PKI, embodiments of the present invention may also provide for authentication of messages across other differing authentication protocols. In embodiments of the present invention, the resource manager utilizes an authentication protocol based on a signature and a public key. However, the authentication protocols used by the client and the middle-tier server, or between the middle-tier server and the public key signature service may be authentication based on a user identification and password, challenge based authentication such as Cryptographic Handshake Authentication Protocol (CHAP) or Digest-MD5, or shared secret based authentication where the parties share a common cryptographic key.

Figure 1 illustrates a network configuration having two different authentication protocols (*e.g.* Kerberos and PKI) in which embodiments of the present invention may be incorporated. As seen in **Figure 1**, a principal may use a client data processing system **10** to request a unit of work from a resource manager, such as the resource server data processing system **20**. Thus, the client **10** and the resource server **20** are endpoints for requesting and providing the work unit respectively. The servers between these endpoints may be referred to as "middle-tier servers." In the exemplary system illustrated in **Figure 1**, the client **10** utilizes a first authentication protocol, such as Kerberos, and the resource server **20** utilizes a second authentication protocol which relies on PKI signatures. The client **10** communicates with a key distribution center **12** and one or more middle-tier servers **14**. The middle-tier servers **14** are delegated authority by the client **10** to act on its behalf in requesting the unit of work from the resource server **20**. Such delegation may be provided by the client **10** obtaining and providing a delegatable credential, such as a delegatable Kerberos ticket, to the middle-tier servers **14**. The middle-tier servers **14** may also obtain delegatable credentials to be forward to the next data processing system in the sequence (tiers) used to reach the resource server **20**.

As is further seen in **Figure 1**, a public key signature service **16** may also be provided. As described in more detail below, the public key signature service **16** receives a delegatable credential from a middle-tier server **14**, verifies the authenticity of the credential and creates a signed message which may be authenticated by the resource server **20** and which contains information about the principal utilizing the client **10** and/or a middle tier server **14** so that the resource server **20** may determine if a requested unit of work is authorized. In PKI embodiments of the present invention, the public key signature service **16** may be trusted by the resource server **20** based on the use of public and private keys and the distribution of certificates by a certificate authority **18**. As is known to those of skill in the art, such public and private keys and certificates may be utilized to uniquely identify the signature of a third party so as to verify the authenticity of information signed by the third party.

While **Figure 1** is illustrated as having a single client **10** and a single resource server **20**, multiple clients and/or servers may also be provided. Furthermore, the middle-tier server **14** is illustrated as communicating with a single resource server **20** but may communicate with one or more resource and/or middle-tier servers. Similarly, multiple key distribution centers, public key signature services and/or certificate authorities may also be provided. Thus, the present invention should not be construed as limited to the configuration of **Figure 1** but is intended to cover all configurations capable of carrying out the operations described herein.

Figure 2 illustrates an exemplary embodiment of a data processing system **230** suitable for providing a client, a middle tier server, a public key signature service and/or a resource server in accordance with embodiments of the present invention. The data processing system **230** typically includes input device(s) **232** such as a keyboard or keypad, a display **234**, and a memory **236** that communicate with a processor **238.** The data processing system **230** may further include a speaker **244**, and an I/O data port(s) **246** that also communicate with the processor **238**. The I/O data ports **246** can be used to transfer information between the data processing system **230** and another computer system or a network. These components may be conventional components such as those used in many conventional data processing systems which may be configured to operate as described herein.

Figure 3 is a block diagram of embodiments of data processing systems that illustrates systems, methods, and computer program products in accordance with embodiments of the present invention. The processor **238** communicates with the memory **236** via an address/data bus **348**. The processor **238** can be any commercially available or custom microprocessor. The memory **236** is representative of the overall hierarchy of memory devices containing the software and data used to implement the functionality of the data processing system **230**. The memory **236** can include, but is not limited to, the following types of devices: cache, ROM, PROM, EPROM, EEPROM, flash memory, SRAM, and DRAM.

As shown in **Figure 3**, the memory **236** may include several categories of software and data used in the data processing system **230**: the operating system **352**; the application programs **354**; the input/output (I/O) device drivers **358**; and the data **356**. As will be appreciated by those of skill in the art, the operating system **352** may be any operating system suitable for use with a data processing system, such as OS/2, AIX or System390 from International Business Machines Corporation, Armonk, NY, Windows95, Windows98 or Windows2000 from Microsoft Corporation, Redmond, WA, Unix or Linux configured to support an TCP/IP-based protocol connection. The I/O device drivers **358** typically include software routines accessed through the operating system **352** by the application programs **354** to communicate with devices such as the I/O data port(s) **246**, the data storage **235** and certain memory **236** components. The application programs **354** are illustrative of the programs that implement the various features of the data processing system **230** and preferably include at least one application which supports operations according to embodiments of the present invention. Finally, the data **356** represents the static and dynamic data used by the application programs **354**, the operating system **352**, the I/O device drivers **358**, and other software programs that may reside in the memory **236.**

As is further seen in **Figure 3**, the application programs **354** may include a public key signature service **360**. The public key signature service **360** may carry out the operations described herein for authenticating messages received in one authentication protocol to provide authenticatable message in a second authentication protocol. The data portion **356** of memory **236**, as shown in the embodiments of **Figure 3**, may include a PKI certificate **364** and a Kerberos ticket **362** received along with a message. The PKI certificate **364** and the Kerberos ticket **362** may be utilized by the public key signature service **360** to authenticate the received message using the two authentication protocols.

While the present invention is illustrated, for example, with reference to the public key signature service **360** being an application program in **Figure 3**, as will be appreciated by those of skill in the art, other configurations may also be utilized while still benefitting from the teachings of the present invention. For example, the public key signature service **360** may also be incorporated into the operating system **352,** the I/O device drivers **358** or other such logical division of the data processing system **230.** Thus, the present invention should not be construed as limited to the configuration of **Figure 3** but is intended to encompass any configuration capable of carrying out the operations described herein.

Operations according to embodiments of the present invention, including operations of the middle-tier server **14**, the public key signature service **16** and the resource server **20,** will now be described with reference to the exemplary network diagram of **Figure 1** and the flowcharts of **Figures 4** through **6**. However, as will be appreciated by those of skill in the art, the network illustrated in **Figure 1** is exemplary only. Embodiments of the present invention may be utilized in other network configurations.

As seen in **Figure 4**, a middle-tier server **14** according to embodiments of the present invention receives a Kerberos ticket (block **400)** and determines if the ticket is delegatable (block **405**). If not, the ticket is processed in a conventional manner (block **430)**. If, however, the ticket is delegatable (block **405**), the middle-tier server **14** obtains a service ticket for the public key signature service **16** from the key distribution center **12** (block **410**). The middle-tier server **14** sends the service ticket and the data to be sent to the resource server **20** to the public key signature service **16** (block **415**) and receives back from the public key signature service **16** a signed message which includes the data sent and an indication of the principal which requested the unit of work (block **420**). The signed message is forwarded to the resource server **20** (block **425**) by the middle-tier server **14**..

Figure 5A illustrates operations of a public key signature service **16** according to embodiments of the present invention. As seen in **Figure 5A**, the public key signature service **16** receives the ticket and the associated data (block **500**) and authenticates the service ticket utilizing the first authentication protocol which, in the present example, is Kerberos (block **505**). The public key signature service **16** creates a new message incorporating the principal information from the service ticket with the data associated with the service ticket (block **510**).

The new message may contain one or more messages or parts. For example, if the data associated with the service ticket is a Secure Socket Layer (SSL) challenge, then the information about the principal may not be incorporated directly with the original data but may be incorporated into a separate identity structure which is associated with the original data and is separately signed by the public key signature service **16**. In such a case, both the data associated with the service ticket and the identity structure could be signed with the digital signature of the public key signature service **16**.

The public key signature service **16** signs the new message with a digital signature utilizing the second authentication protocol (block **515**). The signed message is returned to the middle-tier server from which the service ticket was received (block **520**). Alternatively, the new message could be forwarded directly to the resource server **20**.

Figure 5B illustrates further details regarding operations of the public key signature service **16** according to further embodiments of the present invention. As seen in **Figure 5B**, the public key signature service **16** receives the Kerberos service ticket and the associated data (block **550**) and authenticates the service ticket utilizing the Kerberos protocol (block **555**). If the service ticket is not authentic (block **555**), operations may cease. Alternatively, a log of tickets which fail authentication may be kept for further analysis.

If the service ticket is authentic (block **555**), the principal information is extracted from the ticket (block **560**). Optionally, the public key signature service **16** may also be determined if an identification of the middle-tier server **14** which provided the ticket is to be provided to the resource server **20** (block **565**). If so, the middle-tier information is also extracted from the service ticket (block **570**).

A determination is also made if the principal information and/or the middle-tier server information is to be incorporated with the data associated with the ticket (block **575**). As described above, such a determination may be made based on the type of data associated with the ticket (*e.g.* the unit of work requested by the principal using the client **10**). If additional data cannot be added to the data associated with the ticket, then a separate identity data structure which includes the principal and/or middle-tier server information may be created as a separate component of the message (block **580**). The separate component may be a separate message. If additional data can be added to the data associated with the ticket (block **575**), the principal and/or middle-tier server information and the data associated with the ticket may be incorporated into a message for the resource server **20** (block **585**). In either case, the message and/or messages are signed with the PKI private key of the public key signature service **16** utilizing conventional PKI signature techniques (block **590**) and the signed message(s) returned to the middle-tier server **14** from which the service ticket was received (block **595**). As described above, alternatively, the signed message(s) could be forwarded to the resource server **20** without being returned to the middle-tier server **14** from which the service ticket was received .

Operations of a resource server **20** according to exemplary embodiments of the present invention are illustrated in **Figure 6**. As seen in **Figure 6**, the resource server **20** receives the signed message or messages from the middle-tier server **14** or the public key signature service **16** (block **600**) and determines if the signature is authentic utilizing the second authentication protocol (block **605**). For example, the signature of the message(s) could be verified using conventional PKI techniques.

If the signature is not authentic (block **605**), the data of the message(s) may be rejected (block **635**). If the signature is authentic (block **605**), it may also be determined if the signer of the message(s) was a trusted party (block **610**). If not, the data is rejected (block **635**). If the signer is a trusted party (block **610**), the identity of the requesting principal is obtained from the message(s) (block **615**). It is determined if the requesting principal has the authority to request the unit of work specified by the data (block **620**) and, if not, the data is rejected (block **635**). If the requesting principal has the authority to request the unit of work (block **620**), it may optionally be determined if the middle-tier server **14** is authorized to access the resource server **20** (block **625**) and, if not, the data is rejected (block **635**). If the middle-tier server **14** is authorized to access the resource server **20** (block **625**), the data is processed as if sent by the requesting principal (block **630**). Optionally, if the data is rejected or if the data is processed, an audit log may be updated to indicate the action taken. Such an audit log may record information about the requesting principal.

In addition to the operations described above, optionally, communications with the public key signature service **16** may be encrypted. Furthermore, while the present invention has been described, in part, with reference to the resource server

20, as will be appreciated by those of skill in the art in light of the present disclosure, the resource server **20** is illustrative of resource managers in general. Accordingly, embodiments of the present invention may be utilized to securely access resource managers of differing types. The resource managers may include, for example, security policies for carrying out some or all of the operations described above for authentication of requests to access a resource managed by the resource manager.

The flowcharts and block diagrams of **Figures 1** through **6** illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products for message authentication according to various embodiments of the present invention. In this regard, each block in the flow charts or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be understood that each block of the block diagrams and/or flowchart illustrations, and combinations of blocks in the block diagrams and/or flowchart illustrations, can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

Furthermore, in the drawings, certain operations/acts and or blocks which have been indicated as optional are shown in dashed lines. The presence or lack of such a dashed line shall not, however, be construed as requiring any of the elements of the figures other than those necessary to provide the functions, operations and/or acts specified in the claims set forth below.

In the drawings and specification, there have been disclosed typical illustrative embodiments of the invention and, although specific terms are employed, they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims.